DOJ Component: **Federal Bureau of Investigation**
Total Number of Federal Employees Component-wide: **48,410**
Total Number of Contract Employees Component-wide: **23,387**

# Department of Justice
# Self Inspection Checklist Revision

## Document Security

### A. Original Classification

(Section A applies only to components with Original Classification Authority [OCA])

**1.** Are OCAs familiar with the requirements and overall process for original classification?

- Applicable standards and categories for classification? ○ Y ○ N
- Levels of classification and damage criteria associated with each? ○ Y ○ N
- Avoidance of over-classification? ○ Y ○ N
- Classification prohibitions and limitations? ○ Y ○ N
- Required markings, including those for dissemination and handling? ○ Y ○ N
- Obsolete/invalid markings? ○ Y ○ N
- Determination of declassification instructions? ○ Y ○ N
- Delegations of OCA responsibilities? ○ Y ○ N
- Classification challenges? ○ Y ○ N

**1a.** If **NO** to any of the above requirements and processes, please explain so appropriate education and training tools may be provided. **Click here to enter text.**

2. Do current OCAs have a demonstrable and continuing need to exercise this authority? ◯ Y ◯ N

**2a.** If **YES**, please explain why OCAs have a demonstrable and continuing need.

(U) The 29 current OCAs have a demonstrable and continuing need to exercise original classification authority. Each OCA composes and authorizes classification guides specific to their area of subject matter expertise in order to facilitate classification decisions for all of the different types of information the FBI deals with, i.e., intelligence, Continuity of Operations, information assurance, etc. The OCAs also exercise their authority to facilitate declassification decisions and for information sharing with our IC and Law Enforcement partners, as well as for use in legal proceedings.

(U) Currently the FBI is reviewing the role that OCAs are playing across the FBI. During the next review period, The FBI will research the feasibility of separating the role of OCA from the task of declassifying information.

3. Have OCAs prepared, as appropriate, classification guides to facilitate the proper and uniform derivative classification of information? ◯ Y ◯ N

**3a.** If **NO**, please elaborate why classification guides have not been prepared.
**Click here to enter text.**

4. Do classification guides meet the requirements of Executive Order (EO) 13526, Section 2.2, and 32 Code of Federal Regulations (CFR) Part 2001, Section 2001.15? ◯ Y ◯ N

**4a.** If **NO**, please explain why classification guides do not meet the above requirements.
**Click here to enter text.**

**B.** Derivative Classification

5. Do persons who apply derivative classification markings understand the process and requirements for derivative classification?

- Identity of derivative classifier? ◯ Y ◯ N
- Use of source documents, including classification guides? ◯ Y ◯ N

- Declassification instructions? ○ Y ○ N
- Proper application of markings? ○ Y ○ N
- Portion marking and overall classification marking? ○ Y ○ N
- Classification authority block properly identifying derivative classifiers? ○ Y ○ N
- Obsolete/invalid markings on source documents? ○ Y ○ N

  Multiple sources identified? ○ Y ○ N

- Classification challenges? ○ Y ○ N

**5a.** If **NO** to any of the above requirements and processes, please explain so appropriate education and training tools may be provided.
**Click here to enter text.**

**6.** Do persons who apply derivative classification markings observe original classification decisions and carry classification markings forward to newly created documents? ○ Y ○ N

**7.** Describe the process followed when derivative classifiers identify improper markings on an originally or derivatively classified document. Include actions taken or planned to correct deficiencies or misclassification actions and to deter their reoccurrence.

(U//~~FOUO~~) Those who wish to challenge the classification of FBI information may proceed informally by directly questioning the classifier, or they may submit a formal classification challenge. For Other Government Agency (OGA) information, those who wish to challenge the classification must submit a formal classification challenge. Informal classification challenges may be invoked for derivatively classified FBI information only. (Documents marked "Classified" by an Original Classification Authority (OCA); classification decisions rendered in a classification guide; or classification decisions pertaining to Other Government Agency (OGA) information must be formally challenged. Informally challenged information remains marked at the level it was originally classified, but must be handled and protected at the highest level of classification of the conflicting opinions until the classification conflict is resolved.

(U//~~FOUO~~) When uncertainties exist over the classification status of derivatively classified information, holders of this information are encouraged to make direct contact with the

derivative classifier to correct the classification prior to making a formal classification challenge. Informal classification challenges do not invoke Security Division (SecD) intervention, but challengers may make an informal request to the Strategy, Policy, and Information Security Unit (SPISU), Mission Support Section (MSS), SecD, for guidance and resources to help resolve the dispute.

(U//~~FOUO~~) When approaching a derivative classifier with a classification challenge, the challenger should be prepared to justify the challenge with an OCA's classification determination as conveyed in a classification guide or a properly and accurately marked source document. After the challenger approaches the derivative classifier who originated the document or information, the derivative classifier may either accept the proposed classification correction or may determine that the information should remain marked as is.

(U//~~FOUO~~) If the derivative classifier/originator accepts the proposed classification correction, he or she must create a record copy of the corrected document and, to the most practical extent, notify all holders of the information that the corrected document must be used instead of the incorrectly classified document. The derivative classifier/originator should also record the change, to include the derivative source for the classification, and maintain a record of the change with the file or record copy of the document.

(U//~~FOUO~~) If the derivative classifier/originator determines that the information should remain marked as is, the individual who challenged the classification may not change the marking on the originator's document. If the individual who challenged the classification still believes the information is incorrectly classified and wants to ensure the correct markings are placed on the originator's document, he or she can initiate a formal classification challenge.

(U//~~FOUO~~) Formal classification challenges may be invoked for both originally and derivatively classified information, regardless of agency of origination. Formal challenges are made by filling out the "FBI Formal Classification Challenge Form FD-1061" and submitting it to the SPISU, MSS, SecD. This submission may be either electronic or hard copy. All attempts will be made to resolve challenges within 60 days of receipt by SPISU. If unable to resolve the challenge within 60 days, SPISU shall acknowledge the challenge in writing and provide a date by which a response will be given. The written response will also advise that if no response is given within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP) for a decision.

(U//~~FOUO~~) For challenges to derivatively classified information, SPISU will determine the appropriate classification guide(s) and respective OCA(s) associated with the information and then liaise with that OCA (or his/her subject matter expert designee) to determine the proper marking for the information. All decisions and historical information pertaining to the challenge will be recorded by SPISU.

(U//~~FOUO~~) For challenges to originally classified information, whether an OCA decision conveyed in a classification guide or a document which has been marked "Classified" by an OCA, SPISU will liaise with the OCA who made the decision, as well as any other applicable OCAs (or their subject matter expert designee) to determine the proper classification of the information. The applicable OCA that originally classified the information in question will make the final classification decision.

(U//~~FOUO~~) For challenges to the classification of information originated by another government agency, SPISU will liaise with the proper other government agency (OGA) point of contact to determine proper classification of the information (per the OGA's appropriate OCAs). All decisions and historical information pertaining to the challenge will be recorded by SPISU and a final classification decision will be rendered and conveyed with completion of the FBI Formal Classification Challenge Form FD-1061.

### C. Classified Document Review

(Regular reviews of representative samples of the component's original and derivative classification actions shall be conducted in accordance with 32 CFR Part 2001, Section 2001.60[c][2] to evaluate the classification and marking of the documents)

**8.** How often is a sampling of original and derivative classification actions reviewed? (If **Other**, please explain.)

○ Monthly ○ Bi-annually ○ Annually ○ Other

**Click here to enter text.**

**8a.** Identify what factors are considered in establishing time frame.

(U) This review cycle corresponds to the bi-annual DOJ Security Compliance Review cycle.

**9.** Identify number of documents reviewed as a representative sample.

**636**

**9a.** Are classified documents properly marked, to include documents containing Foreign Government Information, in accordance with the Information Security Oversight Office December 2010, Marking Classified National Security Information Marking Book or agency specific marking guide?

○ Y ○ N

**9b.** In how many classified documents sampled were discrepancies noted?

**80%**

**9c.** List types and number of discrepancies identified during review **(see Attachment 1)**.

**Missing dissemination controls**
**Improper or missing classified by line**
**Missing portion marks**

**9d.** Describe actions taken or planned to correct the discrepancies identified above.

(U) The overwhelming majority of errors identified in the document review were caused by a lack of updates in the WordPerfect templates used by the FBI. With the DOJs impending decommission of WordPerfect the FBI did not expend resources to update the macros used to create investigative documents. In July, 2012 the FBI rolled out Sentinel as the next generation standard for information and case management. The implementation of Sentinel and the inclusion of the Classification Management Tool (CMT) should address the common errors identified with the classification block, portion marking and the missing dissemination controls.

(U) In FY 2013 the FBI will deploy a web based training (WBT) that will cover the basics of working with classified information. This WBT will easily enable more FBI personnel to satisfy the refresher training requirement in Executive Order 13526. The WBT will also free up the resources that were previously dedicated to teaching the basic class to develop more advanced classification training for those employees who need a more specific view of classification beyond the basics.

(U) In addition, The FBI has begun an enhanced communication campaign regarding some of the common errors identified during the document reviews. Three Security Bulletins have been drafted to address the use of portion marks, classification by compilation and the use of ORCON. Others will be drafted throughout the next review period as topics are identified.

**9e.** How many documents reviewed were derivatively classified documents?
**636**

1. What percent of derivatively classified documents contained derivative classifier's name and position, or personal identifier?
   **26%**

**9f.** How many derivatively classified documents reviewed were derived from multiple sources?

(U) Unknown. The FBI review was based on the DOJ checklist from 2011 which did not request this statistic. The FBI will begin tracking this for the 2013 report.

**1.** What percent of these documents had a list of sources included or attached?
**0**

**D. Security Education**
(OCAs are required to receive training in proper classification and declassification each calendar year.)

**10.** How many OCAs exist within the component? **29**

**10a.** What percentage of OCAs received initial OCA training prior to originally classifying information? **100%**

**10b.** What percentage of OCAs have received annual OCA refresher training?

(U) Due to the constant change in executive management assignments, the current percentage of OCAs that have received annual refresher training is 72%. (21 out of 29) According to new OCA Policy, OCAs must complete OCA training within 30 days of assuming the OCA-delegated position, complete OCA training annually, and complete OCA training prior to rendering OCA decisions. All remaining OCAs are being scheduled for their annual refresher.

**10c.** Have any waivers to this requirement been granted?
**No**

(Derivative classifiers are required to receive training in the proper application of the derivative classification principles of EO 13526 prior to derivatively classifying information and at least once every two years thereafter.)

**11.** How many derivative classifiers exist within the component?
**48,410**

**11a.** What percentage of derivative classifiers have received initial derivative classification training prior to derivatively classifying information?
**1.6%**

**11b.** What percentage of derivative classifiers have received refresher training within the past two years? **18.5%**

**11c.** Have any waivers to this requirement been granted?

**No**

(All cleared personnel are required to receive initial training on basic security policies, principles, practices; and criminal, civil, and administrative penalties. Agencies are required to provide annual refresher training to all employees who create, process, or handle classified information. Cleared personnel who leave the Department or whose clearance has been withdrawn or revoked is required to receive a termination briefing.)

**12.** How many cleared federal employees exist within the component?

**48,410**

**12a.** What percentage of cleared federal employees receive initial training?

**1.6%**

**12b.** What percentage of cleared federal employees receive refresher training?

**18.5%**

**13.** How many cleared federal employees left the Department or had a clearance withdrawn or revoked in the past year? **1,191**

**13a.** What percentage of these cleared federal employees received a termination briefing?

**(U) Unknown - The FBI tracks the if briefings are given; a special query must be built to answer how many were done**

**14.** Are authorized couriers of classified information briefed on their responsibilities? ○ Y ○ N

**15.** Are records kept of the various training and briefings provided and the employees who participated? ○ Y ○ N

**E.** Declassification

**16.** Describe the records management system facilitating public release of declassified documents.

(U) The purpose of the FBI, Records Management Division (RMD), Record/Information Dissemination Section (RIDS) is to effectively plan, develop, direct and manage responses to

requests for access to FBI records and information. The requests and disclosures comply with the Freedom of Information and Privacy Acts (FOIPA), Title 5, United States Code, Sections 552 and 552a; the Mandatory Declassification Review (MDR) provisions of Executive Order 13526; Presidential, Attorney General, and FBI policies and procedures; judicial decisions; and other Presidential and Congressional directives. RIDS efforts are directed to appropriately release information in an efficient and effective manner while protecting legitimate law enforcement, foreign policy, national security, and defense interests. To date in FY 2012, the FBI has received approximately 20,000 FOIPA and other access requests from the public. RIDS has reviewed at least 1.2 million pages pursuant to these requests. FOIPA and other requests are processed in an electronic case management and redaction system which promotes the efficient processing and release of declassified non-exempt information to the public. Responses to requests can be provided to the requester in paper or in an electronic format.

(U) To facilitate public access to declassified and other non-exempt information, RIDS maintains a public website known as "The Vault." Thus far in FY 2012, "The Vault" has received 3,260,890 views. The website contains 3.5 terabytes of historically significant information on 500 different subject matters. The accessibility of information on "The Vault" has received significant positive feedback from the requester community, the media, and the general public.

(U) Additionally, RIDS conducted declassification reviews on over 1.2 million pages of permanently valuable classified records aged 25 years and older pursuant to the systematic declassification provisions of Executive Order 13526. Many of these reviewed pages will be transferred to the National Archives where they will undergo archival processing for eventual availability to the public.

**17.** Describe procedures established for automatic, systematic, discretionary, and mandatory declassification review.

(U) FBI/RMD/RIDS is responsible for declassification reviews conducted under the automatic, systematic, discretionary, and mandatory declassification review provisions of Executive Order 13526. While conducting these reviews, RIDS ensures information which no longer meets the criteria for classification established by FBI Classification and Declassification guides is declassified, and information which continues to meet the criteria for classification remains classified.

(U) For all types of declassification reviews, regardless of whether they are automatic, systematic, discretionary, or mandatory, RIDS follows the same general methodology for conducting a review. Each classified record is evaluated using the following process:

First, determine the originator of the classified information.

- Classified information which originates with another agency will be forwarded to that agency so it can make classification determinations on its information.

Next, determine the age of the information.

- When the information is aged 25 years or older, but less than 50 years old, the Appendices of the FBI Automatic Declassification Guide (ADG) must be consulted to determine whether the information is from an automatic-declassified file series or an exempt file series.

- When it is determined the information originates from an automatic-declassified file series, the review is conducted with the understanding that the information is declassified.

- Even if declassified, there will be cases when the information should not have been automatically declassified because it meets one or more of the criteria for exemption from automatic declassification listed in the ADG. In such instances, the information must be reclassified using the processes directed by Executive Order 13526 and Department of Justice procedures.

- If the information does not meet the criteria for reclassification, it shall remain declassified.

- If it is determined the information originates from an exempt file series, each unique category of classified information shall be evaluated to determine if the information continues to be exempt from automatic declassification pursuant to the specific exemption codes listed in the ADG.

- Classified information which, pursuant to the ADG, no longer meets the criteria for exemption from automatic declassification shall be declassified.

- When the classified information is aged 50 years or older, the review is no longer based on exempt versus declassified file series. Instead, the information shall be evaluated to determine whether the information continues to be eligible for exemption from automatic declassification pursuant to those portions of the ADG which implement Section 3.3(h)(2) of Executive Order 13526.

- The three categories of information which can be considered for exemption from automatic declassification at 50 years of age are:

The identity of a confidential human source or human intelligence source;
Key design concepts of weapons of mass destruction; and
"Extraordinary cases" (a classified description of the FBI's "extraordinary case" is available in the ADG).

- Classified information which, pursuant to the ADG, no longer meets the criteria for exemption from automatic declassification shall be declassified.

- When the information is not yet aged 25 years or older, it must be evaluated to determine if any of the information continues to be classified pursuant to the National Security Information Classification Guide and/or other appropriate FBI classification guides. This evaluation often relies on the input from FBI operational components.

- Classified information which, pursuant to applicable guides, no longer meets the criteria for classification shall be declassified.

**F.** Safeguarding

**18.** Is all classified material properly protected in accordance with 32 CFR Part 2001,Subpart D and the Department of Justice (DOJ) Security Program Operating Manual (SPOM), Chapter 6?

- Do you have a system of control measures which assures access to classified information is limited to authorized persons? (Y) N
- Do you have a system of control measures which deter and detect access by unauthorized persons? (Y) N
- Is classified material stored in General Services Administration (GSA) approved security containers or Department Security Officer (DSO) approved open storage areas? (Y) N
- Is Top Secret information stored in a GSA-approved security container along with proper supplemental controls? (Y) N
- Are combinations safeguarded the same as the highest level of classified information being protected? (Y) N
- Are combinations changed only by persons authorized access to the highest level of information stored in the container? (Y) N
- Do you use Standard Form (SF) 700s "Security Container Information"? (Y) N
- Do you have Confidential or Secret information protected by a key operated lock? (If **NO**, proceed to next bullet) Y (N)
  - Has the key operated lock been approved by the DSO? Y N
  - Have administrative procedures for control and accounting of keys and locks been established? Y N
- Is classified information kept under constant surveillance and covered to prevent unauthorized access when removed from storage for working purposes? (Y) N

- Is a system of security checks or inspection implemented at the close of each business day to ensure classified information is properly secured? ○ Y ○ N
  - Are SF 702s "Security Container Check Sheets" utilized? ○ Y ○ N
  - Are SF 701s "Activity Security Checklist" utilized? ○ Y ○ N
- Does the official responsible for arranging a conference or meeting institute ensure adequate security is provided if classified information is to be discussed? ○ Y ○ N
  - Are meetings held only in a U.S. Government facility or at a cleared facility of a DOJ contractor or consultant? ○ Y ○ N
  - Are attendees notified of imposed security limitations due to attendees' access level authorizations or physical security conditions of the facility? ○ Y ○ N

**19.** Is all classified material transmitted in accordance with 32 CFR Part 2001, Section 2001.45 and the DOJ SPOM, Chapter 6-500?

- Is classified information physically transmitted outside the facility in two opaque layers? ○ Y ○ N
- Is authorization to hand-carry classified information between DOJ components and other organizations only given to DOJ personnel appropriately briefed and authorized in writing by the SPM? ○ Y ○ N

**20.** Is all classified material reproduction in accordance with 32 CFR Part 2001, Section 2001.44 and the DOJ SPOM, Chapter 6-402?

- Held to a minimum consistent with operational requirements? ○ Y ○ N
- Accomplished only by authorized persons knowledgeable of the procedures for classified reproduction? ○ Y ○ N
- Accomplished only with approved equipment? ○ Y ○ N
- Appropriate procedures for reproduction of classified information posted on or near equipment approved for such reproduction? ○ Y ○ N

**21.** Is all classified material destroyed in accordance with 32 CFR Part 2001, ○ Y ○ N

Section 2001.46 and the DOJ SPOM, Chapter 6-600?

If **NO** to **18-21**, please explain further.

The FBI uses X-09 combination locks on all containers used to store classified information.

**G. Telecommunications, Automated Information Systems (IT), and Network Security**

**22.** Consistent with EO 13526, Section 4.1; 32 CFR Part 2001, Section 2001.50; and the DOJ SPOM, Chapter 8, describe uniform procedures established to ensure automated information systems that collect, create, communicate, compute, disseminate, process or store classified information are protected in accordance with applicable national policy issuances.

(U) The FBI Certification and Accreditation (C&A) process supports the goal of the FBI Information Assurance Program to protect National Security Information (NSI) and the Information Systems (IS) processing that information. In order to attain this goal, the FBI's Information Assurance (IA) program includes elements that:

- Ensure all individuals with access to classified or sensitive information [e.g. For Official Use Only (FOUO), Sensitive But Unclassified (SBU), Law Enforcement Sensitive (LES)] or FBI ISs that process classified or sensitive information have the proper security clearance, formal accesses, need-to-know, and training.
- Ensure the Confidentiality, Integrity, and Availability of information processed by FBI ISs.
- Protect the FBI's Enterprise through the infusion of security technology and appropriate oversight.
- Establish a comprehensive, consistent, and centrally managed IA Program that institutes full lifecycle security.

(U) The FBI implements the security authorization process, as defined in the C&A Handbook, to determine Information System's compliance with the goals stated above and the controls outlined in the Information System Security Framework Policy. This policy defines the minimum baseline IS security controls to ensure that the confidentiality, integrity, and availability of the FBI's computer systems, networks, and information are maintained. These information assurance standards, including those contained in the associated appendices of the Information Systems Security Framework Policy, are used to consistently identify and to select applicable security controls to secure FBI ISs based on assessed risks.

**23.** Describe procedures implemented to prevent unauthorized access, ensure the integrity of the information, and maximize the accessibility of information to persons who meet the criteria set forth in EO 13526, Section 4.1(a).

(U) The FBI Certification and Accreditation (C&A) process supports the goal of the FBI Information Assurance Program to protect National Security Information (NSI) and the ISs processing that information. In order to attain this goal, the FBI's Information Assurance (IA) program includes elements that:

- Ensure all individuals with access to classified or sensitive information (e.g. For Official Use Only (FOUO), Sensitive But Unclassified (SBU), Law Enforcement Sensitive (LES)) or FBI ISs that process classified or sensitive information have the proper security clearance, formal accesses, need-to-know, and training.
- Ensure the Confidentiality, Integrity, and Availability of information processed by FBI ISs.
- Protect the FBI's Enterprise through the infusion of security technology and appropriate oversight.
- Establish a comprehensive, consistent, and centrally managed IA Program that institutes full lifecycle security.

(U) The FBI implements the security authorization process, as defined in the C&A Handbook, to determine Information System's compliance with the goals stated above and the controls outlined in the Information System Security Framework Policy. This policy defines the minimum baseline IS security controls to ensure that the confidentiality, integrity, and availability of the FBI's computer systems, networks, and information are maintained. These IA standards, including those contained in the associated appendices of the Information Systems Security Framework Policy, are used to consistently identify and to select applicable security controls to secure FBI ISs based on assessed risks.

**24.** Do all IT systems that process, store, or handle classified information meet the requirements in the DOJ SPOM, Chapter 8? ○ Y ○ N

**24a.** If **NO**, please explain. **Click here to enter text.**

**25.** Are all IT system components having the potential to retain classified information marked with the highest classification level and most restrictive classification category? ○ Y ○ N

**25a.** If **NO**, please explain. **Click here to enter text.**

**26.** Is all data introduced on a classified IT system the same or lower security classification level for which the IT system is approved to operate? ○ Y ○ N

**H.** Security Violations

(All security violations are required to be reported to the Department Security Officer.)

**27.** Is the loss, possible compromise, or unauthorized disclosure of classified ○ Y ○ N

information appropriately reported in accordance with the DOJ SPOM, Chapter 1-300?

**27a.** Are personnel familiar with the reporting procedures? (Y) N

**27b.** What procedures are implemented to conduct an inquiry/investigation?

(U) In 2003, the Security Compliance Unit (SCU) was established to oversee and manage the Security Incident Program. When an individual has committed or becomes aware of a security incident, he/she reports the incident to his/her respective Chief Security Officer (CSO). CSOs have the responsibility to conduct an inquiry into the incident in order to resolve all security concerns. CSOs are also responsible for reporting the incident to SCU as the entity responsible for ensuring all reported incidents are documented, investigated and mitigated.

**27c.** Are appropriate and prompt corrective actions taken when a security violation or infraction occurs? Describe process. (Y) N

(U) In addition to the above, in 2009 the FBI implemented the Security Incident Reporting System (SIRS), which is a central database to capture all security incidents reported by employees and personnel associated with the FBI (i.e. contractors, taskforce members). Upon notification of an incident, SCU works closely with field and HQ CSOs, and other entities as necessary, to ensure the incident is properly investigated/mitigated in a timely manner. As part of the mitigation of incidents, CSOs are held responsible for conducting awareness briefings and providing training on security policy and procedures to an individual who commits a security incident. In addition, SCU ensures that all parties that may have a vested interest in reported security incidents are notified. Referrals made by SCU include, but are not limited to:

- Inspection Division – potential misconduct
- Office of General Counsel- potential breach of Personally Identifiable Information
- Counterintelligence Division – potential espionage matters
- Enterprise Security Operations Center – Information Technology related incidents

**27d.** Are individuals who commit violations or infractions subject to appropriate sanctions? (Y) N

**I.** Management and Oversight

**28.** How many personnel are dedicated to manage the classified national security information program? **26**

**29.** Are sufficient resources and personnel committed to implement the classified national security information program? If **NO**, please explain. Y (N)

(U) More resources are necessary to provide in person training and to address questions regarding classification of NSI. Additional resources are also necessary to conduct document reviews and to address training issues identified as a result of security compliance reviews and document reviews.

(U) Additionally, in anticipation of a change of administration, more resources will be needed to address new executive orders related to NSI and the associated training.

**30.** Describe how security personnel fulfill responsibilities to implement the program.

(U) All members of the FBI's Information Security Team (IST) are qualified to train how to identify, designate and mark classified national security information. In FY 2012 alone, 4,665 FBI personnel were trained. The trainers traveled to field offices, and offered recurring training at FBIHQ. In addition, all New Agent Trainees, Intelligence Analysts and Staff Operations Specialists receive training on working with classified information during their initial training. Training is also provided to Joint Terrorism Task Force Officers, Chief Reports Officers and Legal Attaché Staff before reporting to their positions. A WBT will be deployed on the FBI's Virtual Academy in early FY 2013. With the deployment of this application, the trainers will be freed up to implement a more advanced training, and the basic training will be more available to a wider audience across all of the FBI.

(U) In FY 2012, the InformationSecurity Oversight Program (ISOP) began conducting document reviews. These reviews are conducted along with the Security Compliance Reviews and the DOJ Security Compliances Reviews. In FY 2013 4 DOJ reviews are scheduled and 15 Security Compliance Reviews are scheduled. The ISOP personnel are scheduled to travel to field offices and conduct the information security portions of the reviews.

(U) The IST members also conduct analysis to determine if new or updated information security policies are necessary. Occasional reviews of executive orders and existing policies are conducted to ensure that all policy guidance is relevant, consistent and up to date.

(The performance contract or other rating system of OCAs, security managers, and other personnel whose duties significantly involve the creation or handling of classified information must include a critical element to be evaluated relating to designation and management of classified information.)

**31.** How many personnel fit within the categories identified above?

**0**

**31a.** What percentage of such personnel at your component has this element in their performance contracts? **0**

**32.** How many cleared contract employees exist within the component?
**23,387**

---

**Please include the following information in your report to the Department Security Officer on the results of your self-inspection:**

1. A description of the component's self-inspection program to include the criteria identified below. The description should demonstrate how the self-inspection program provides the senior agency official with information necessary to assess the effectiveness of the classified national security information program within the component as a whole (Headquarters/ Division/District/Field/Resident/Satellite/Overseas offices).

    - Who conducts the self inspections;
    - Activities assessed;
    - Program areas covered; and
    - Methodology utilized.
        - Means and methods employed;
        - Different types of self inspections conducted (interviews with producers and users of classified information, reviews of representative samples).
        - Include how component headquarters gather information from the various offices, e.g., Division/District/Field/Resident/Satellite/Overseas offices.

(U) The ISOP is located in the SPISU, MSS, SecD. The ISOP is responsible for all information security reporting required by agencies outside for the FBI. The ISOP also conducts onsite document reviews of needed for these reports. The ISOP personnel conducted six document reviews in 2012 and plan to do 15 onsite document reviews in 2013.

(U) The review methodology consisted of a random selection of 25 pending file volumes, and 25 closed file volumes for the previous 2 years, and were reviewed by the reviewer at the Field office. All volumes contained classified information. The criteria for the review were based on the 2011 DOJ checklist. If discrepancies there were consistent, an issue was identified for future action including Security Bulletins and training issues.
Criteria included details regarding:

- Banner lines
- Portion Markings
- Classification Authority Block
- Proper "Classified By" line
- "Derived from" line (if applicable)

- Declassification Instructions
- List of sources (if applicable)
- Dissemination Controls
- Markings uniformly and conspicuously applied
- The review only addressed documents created by the field office under review. (No foreign documents and nothing from HQ or other field entities)
- A checklist was completed for each document reviewed, including identification of serial and file number at the top of the sheet and comments if applicable.
- The ISOP will continue to explore the use of the audit capabilities in Sentinel in future reviews to address a wider sample of FBI originating documents.
- The review was not intended to determine if the information is classified at the correct level, only to determine the presence and agreement of the basic elements of classification.
- Based on available funding, the ISOP will continue to conduct onsite reviews of documents. It is anticipated that between onsite reviews and available auditing capabilities of FBI IT that a more representative sample of FBI generated classified documents will be obtained in future years.

2. Identify best practices that were identified during self-inspections.

(U) Best practices identified during the self-inspection include:

- Continue onsite reviews and document reviews using IT system audit capabilities (Sentinel and CMT)
- Effective September 30, 2012, the DOJ is decommissioning WordPerfect. The FBI was the only element of the Intelligence Community still using WordPerfect; therefore, no resources were committed to updating classification templates or modifying the Classification Management Tool (CMT).
- The CMT is a commercial off the shelf tool that works with most Microsoft office products. It was originally created by the CIA. It is compliant with all CAPCO classification policies. A version is available on FBI's Sentinel and all FBI Microsoft desktop applications.
- The FBI will deploy a basic classification WBT that will be able to satisfy the refresher training requirement for most FBI employees.
- Based on available funding, in person training will continue in the field and recurring training continues at headquarters and other DC metro locations
- The IST will continue to publish Security Bulletins on common information security errors and disseminate them to the entire FBI.

**ATTACHMENT 1**
**EXPLANATION OF DISCREPANCIES**

**OVERCLASSIFICATION**: (a) Clear-cut: The information in the document does not meet the standards necessary for classification; (b) Questionable: While the question of meeting classification standards is arguable, classification does not appear to be necessary to protect our national security; (c) Partial: A portion(s) of the document appear(s) to be unnecessarily classified, although the overall classification of the document is correct.

**OVERGRADED**: All or some of the information in the document appears to be classified at a higher level than justified.

**UNDERGRADED**: All or some of the information in the document appears to be classified at a lower level than necessary.

**DECLASSIFICATION**: The document has improper or incomplete declassification instructions or no declassification instructions.

The "Declassify on" line should contain one of the following:
(1) a date or event less than 10 years from the date the information/document was created;
(2) a date 10 years from the date the information/document was created;
(3) a date greater than 10 years and less than 25 years from the date the information/document was created;
(4) a date 25 years from the date the information/document was created;
(5) 25X1–25X9, with a date or event of declassification, provided that the classifying agency has received approval from the Interagency Security Classification Appeals Panel (ISCAP) to exempt the information;
(6) 50X1–50X9, with a date or event of declassification, provided that the classifying agency has received approval from the ISCAP to exempt the information;
(7) 50X1-HUM or 50X2-WMD, provided that the ISCAP has been informed of the agency's intent to use this marking; or
(8) 25X1, E.O. 12951, provided that the document contains space-based imagery.

Other markings, such as "OADR" and X1–X8, are not valid under the current Order, and "MR," "DCI/DNI Only," and "Subject to International Treaty or Agreement" have never have been valid declassification markings. See 32 C.F.R. Part 2001 and/or the ISOO booklet, "Marking Classified National Security Information," for further details.

When declassification dates are displayed numerically, the following format must be used: YYYYMMDD.

**DURATION**: A lesser duration of classification appears more reasonable.

**UNAUTHORIZED CLASSIFIER (Unknown Basis for Classification)**: The document appears to have been classified by someone not authorized to do so.

**"CLASSIFIED BY" LINE – Original Classification (Unknown Basis for Classification)**: The document does not identify the OCA by name and position or by personal identifier. If the identification of the originating agency or office is not apparent on the face of the document, it should be listed below the position.

**"REASON" LINE**: An originally classified document does not include the "Reason for Classification," or it cites an incorrect category from section 1.4 of the Order. A "Reason" line does not appear on a derivatively classified document, and if included is cited as a discrepancy.

**"CLASSIFIED BY" LINE – Derivative Classification (Unknown Basis for Classification)**: The document does not identify the derivative classifier by name and position or by personal identifier.

**ATTACHMENT 1**
**EXPLANATION OF DISCREPANCIES**

**"DERIVED FROM" LINE (Unknown Basis for Classification)**: The document fails to cite, or cites improperly, the classification source. The line should include type of document, date of document, subject, and office/agency of origin.

**MULTIPLE SOURCES(Unknown Basis for Classification)**: The document cites "Multiple Sources" as the basis for classification, but does not list these sources.

**ORIGINAL/DERIVATIVE**: The document is marked and treated as an original classification action although the classified information appears to be derived from a guide or other source(s).

**MARKING**: The document lacks overall classification markings or has improper overall classification markings (e.g., lacks the highest overall marking, contains erroneous overall markings, or lacks overall markings and/or caveats on transmittal documents).

**PORTION MARKING**: The document lacks required portion markings.